

**CLAIMS**

What is claimed is:

- 1           1.       A method of providing security for a computer system, the method comprising  
2   the acts of:  
3       generating a request for a file;  
4       receiving the request at a dedicated security processor;  
5       using the dedicated security processor to access the file;  
6       using the dedicated security processor to validate the requested file; and  
7       providing the file to an other processor, if the requested file is validated.
- 1           2.       The method, as set forth in claim 1, comprising the act of validating a user  
2   access to execute the request.
- 1           3.       The method, as set forth in claim 2, comprising the act of responding to the  
2   other processor with an abort message if the user access is invalid.
- 1           4.       The method, as set forth in claim 2, comprising the act of enabling the other  
2   processor to continue processing the file, if the user access is validated.
- 1           5.       The method, as set forth in claim 1, comprising the act of disabling the other  
2   processor once the file is requested and enabling the other processor to continue processing  
3   after the requested file is validated.
- 1           6.       The method, as set forth in claim 1, wherein accessing the file comprises  
2   loading the file from a system memory.

1           7.     The method, as set forth in claim 1, wherein accessing the file comprises  
2 loading a memory resident file.

1           8.     The method, as set forth in claim 1, wherein the dedicated security processor is  
2 in a remote computer system.

1           9.     The method, as set forth in claim 1, wherein the other processor and the  
2 dedicated security processor are disposed in a computer system.

1           10.    The method, as set forth in claim 1, comprising the act of setting a return  
2 status field to valid, if the requested file is valid.

1           11.    The method, as set forth in claim 1, wherein the act of generating the request  
2 comprises the acts of:  
3                setting a semaphore;  
4                forwarding the semaphore to the dedicated security processor; and  
5                blocking further processing of the file, if the semaphore is not set to a specific  
6                setting.

1           12.    The method, as set forth in claim 1, wherein the act of validating the requested  
2 file comprises the act of accessing a database for a digital signature of the file being  
3 requested.

1           13.     The method, as set forth in claim 12, wherein the act of validating the  
2 requested file comprises the act of calculating a secure hash and comparing the calculated  
3 secure hash to a stored secure hash.

1           14.     The method, as set forth in claim 1, wherein the act of validating the requested  
2 file comprises the act of accessing a database for an error checking and correction ("ECC")  
3 code corresponding to the requested file.

1           15.     The method, as set forth in claim 14, wherein the act of accessing the database  
2 comprises the act of correcting the file by utilizing the ECC code corresponding to the  
3 requested file.

1           16.     A method of providing security for a computer system, the method comprising  
2 the acts of:  
3           generating an identifying number from a security processor;  
4           providing the identifying number to an other processor in the computer system;  
5           incorporating the identifying number into a request for a file;  
6           delivering the request to the security processor;  
7           using the security processor to access the file;  
8           using the security processor to validate the requested file;  
9           verifying the identifying number at the security processor; and  
10          providing the file, if the requested file is validated and the identifying number is  
11 verified.

1           17.     The method, as set forth in claim 16, comprising the act of enabling the other  
2     processor to continue the processing, if the identifying number is validated.

1           18.     The method, as set forth in claim 16, comprising the act of terminating the  
2     access if the identifying number is invalid.

1           19.     The method, as set forth in claim 16, wherein the security processor is in a  
2     remote computer system.

1           20.     The method, as set forth in claim 16, wherein the other processor and the  
2     security processor are disposed in the computer system.

1           21.     The method, as set forth in claim 16, wherein the identifying number is a  
2     nonce.

1           22.     The method, as set forth in claim 16, wherein the identifying number is a  
2     time stamp.

1           23.     The method, as set forth in claim 16, wherein the act of validating the  
2     requested file comprises the act of accessing a database for an error checking and correction  
3     ("ECC") code corresponding to the requested file.

1           24.    A computer system comprising:  
2                means for validating a file at a security processor, wherein the means for validating  
3                the file comprises:  
4                means for storing a record in a memory used to validate the file;  
5                means for verifying the record against the file at the security processor; and  
6                means for indicating that the file is verified to an other processor.

1           25.    The system, as set forth in claim 24, comprises means for validating a user  
2                access.

1           26.    The system, as set forth in claim 24, wherein the means for verifying  
2                comprises:  
3                means for storing a public key and a hash algorithm used to validate the file;  
4                means for storing an encrypted hash correlative to the requested file in the record; and  
5                means for comparing the record with the requested file.

1           27.    The system, as set forth in claim 24, comprises means for verifying an  
2                identifying number in a request at the security processor.

1           28.    A networked computer system comprising:  
2                a plurality of computer systems;  
3                a network coupled to each of the plurality of computer systems;  
4                at least one of the plurality of computer systems comprising:  
5                a first processor;

6           a security processor operatively coupled to the first processor;  
7           a first section of memory configured to store a file, the first section of memory  
8       being operatively coupled to the first processor and the security processor; and  
9           a second section of memory being configured to store a validation program  
10       that is initiated by the security processor, the validation program having a validation  
11       routine configured to validate the file stored in the first section of memory when the  
12       security processor receives a request for the file, and the validation program using an  
13       encrypted code to validate the file.

1           29.     The system, as set forth in claim 28, wherein a second processor in a second of  
2       the plurality of computer systems is adapted to utilize the security processor for validating the  
3       file.

1           30.     The system, as set forth in claim 29, wherein the memory is a memory resident  
2       file.

1           31.     The system, as set forth in claim 28, wherein the request comprises a  
2       semaphore and an address for the semaphore, wherein the semaphore blocks the processor  
3       from executing the file, if the semaphore is set in a specified manner.

1           32.     The system, as set forth in claim 28, wherein a second processor in a second of  
2       the plurality of computer systems is adapted to generate a request for the file from the security  
3       processor and is adapted to receive the validated file from the security processor.